MILITARY HEALTH SYSTEM (MHS)	**IMPLEMENTATION GUIDE No. 7**	
INFORMATION ASSURANCE (IA) **IMPLEMENTATION GUIDE**	**EFFECTIVE DATE** 07/19/05	**REVISED DATE** xx/xx/xx

Subject:

DATA INTEGRITY

1 PURPOSE AND SCOPE

The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

The term "MHS Information System (IS)" encompasses all automated IS applications, enclaves, outsourced IT-based processes, and platform information technology (IT) interconnections as defined in DoD Instruction (DoDI) 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

This implementation guide outlines safeguards for detecting and minimizing inadvertent modification or destruction of data. Data integrity is a security principle that ensures the continuous accuracy of data and information stored within networked systems. Data integrity is defined as the condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. Continuity of data integrity is paramount in the MHS IS environment and is a key concept of the Defense-in-Depth strategy. System integrity is defined as the attribute of an IS when performing its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Data must be kept from unauthorized modification, forgery, or any other form of corruption, such as from malicious threats or corruption that is accidental in nature.

Upon receiving and processing Sensitive Information in an MHS IS, integrity must be verified to ensure that the information has not been altered, modified, or added to or subtracted from in transit by unauthorized users. Integrity has two main objectives:

a. Ensure that the data has not been altered in an unauthorized manner while in transit, during storage, or while being processed.

b. Ensure that a system, while performing its intended processes and applications, provides support to authorized users free from unauthorized manipulation.

Exploitation of vulnerabilities associated with data or system integrity may result in a disruption or denial of service, and/or unauthorized modification of user or network information and network services. Data and system integrity requires implementing protection mechanisms as a means of preventing unauthorized modification or destruction of information. It is the responsibility of the MHS IA Program Office to ensure protective measures are in place, coupled with industry best practices, to maintain the appropriate level of data and system integrity.

2 POLICY

MHS requires implementing data and system integrity measures to protect DoD data from unauthorized manipulation, intentional or unintentional alteration, or destruction. Instituting access control mechanisms, utilizing virus protection programs, and establishing an information security monitoring capability are required measures, in accordance with Defense-in-Depth, to help protect the integrity of DoD data and systems.

It is MHS Policy that:

2.1 The Information Assurance Officer (IAO) shall ensure that access to all DoD and MHS information is determined by its classification, sensitivity, and need-to-know. Need-to-know is established by the information owner and is enforced by discretionary or role-based access controls.

2.2 The IAO shall ensure policies and procedures are implemented for ISs that handle DoD data to allow access only to those persons or software programs that have been granted access rights.

2.3 The IAO shall establish and enforce access controls for all shared or networked file systems and internal Web sites, whether classified, sensitive, or unclassified.

2.4 All internal classified, sensitive, and unclassified Web sites shall be organized to provide at least three distinct levels of access:

a. Open Access – General information made available to all DoD and TMA Component authorized users with network access. This access does not require an audit transaction.

b. Controlled Access – Information made available to all DoD and TMA Component authorized users upon the presentation of an individual authenticator. This access shall be recorded in an audit transaction.

c. Restricted Access – Need-to-know information made available only to an authorized community of interest. Authorized users must present an individual authenticator and have a demonstrated or validated need-to-know. All access to need-to-know information and all access attempts shall be recorded in audit transactions.

2.5 The IAO shall establish appropriate control mechanisms to ensure that data at rest or in transit is properly disposed of by authorized personnel only.

2.6 The IAO shall establish and enforce procedures to verify the identity of a person or entity seeking access to data.

2.7 The IAO shall maintain and enforce procedures to establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

2.8 The IAO shall ensure that a controlled interface is implemented for interconnections among DoD ISs operating at different classifications levels or between DoD and non-DoD systems or networks.

2.9 The IAO shall determine the need for and the strength of the mechanism for automatic logoff based on DoD direction and the organization's risk assessment, and shall document policies and procedures for terminating an electronic session after a predetermined time of inactivity.

2.10 The IAO shall determine the appropriate mechanism for encrypting and decrypting sensitive electronic data and protected health information at rest and in transit in accordance with Federal Information Processing Standards (FIPS) 140-2, "Security Requirements for Cryptographic Models," dated December 3, 2002 and DoDI 8500.2.

2.11 The IAO shall implement system resource control and object access to ensure that all authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object released back to the system. There must be no residual data from the former object.

2.12 The IAO shall implement electronic mechanisms to confirm that data has not been altered or destroyed in an unauthorized manner.

2.13 Virus protection shall be installed, enabled, maintained, and have the ability to be automatically updated on all MHS ISs.

2.14 TMA Components shall review system records on a weekly basis, or more frequently if deemed necessary.

2.15 TMA Components shall implement and maintain an information security monitoring capability to ensure that all systems they operate and/or control are regularly monitored and protected by intrusion detection systems.

2.16 Successive logon attempts shall be controlled using one or more of the following:

a. Access is denied after three unsuccessful logon attempts in accordance with Chairman, Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND)," dated March 25, 2003.

b. The number of access attempts in a given period is limited.

c. A time-delay control system is employed.

d. The system provides a capability to control the number of logon sessions if the system allows for multiple-logon sessions for each User Identification (User ID).

3 PROCEDURES

3.1 The IAO shall manage authorized user accounts for MHS systems, including configuring access controls to enable access to authorized information and removing authorization when access is no longer needed. The responsibility may be delegated to the System Administrator.

3.2 Limit users to three attempts when logging onto an MHS IS. After the maximum number of incorrect attempts, the system shall lock out the user until an administrator unlocks the account. Action from the IAO shall be required to reactivate the account. This action prevents outsiders from accessing the IS by using a known User ID and trying to guess the password.

3.3 Enable screen-lock functionality on all MHS workstations and any workstation that accesses DoD information. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, hiding what was previously visible. Such a capability is enabled by either explicit user action or a specified period of workstation inactivity (e.g., fifteen minutes). Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator.

3.4 The screen lock function shall not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

3.5 In addition to DoD 5500.7-R, “Joint Ethics Regulation (JER),” requirements, the Health Insurance Portability and Accountability Act Security Rule provides specific security standards for the protection of workstations that process protected health information. These include:

a. Locking the workstation before leaving the workstation unattended.

b. Position workstation to obstruct unauthorized viewing and access.

3.6 The IAO shall establish Web site administration policy and procedures consistent with the “DoD Web Site Administration Policies and Procedures,” November 25, 1998, as amended on January 11, 2002.

3.7 The IAO shall establish system Access Control Lists to restrict traffic to only that which is required to pass through the Web site.

3.8 All MHS IS users shall take precautions to prevent viruses from infecting MHS ISs. The IAO shall ensure all developers are protecting source or executable code by utilizing ‘checksum’ or another safeguard to ascertain that approved code is not altered.

3.9 The IAO shall ensure all software loaded on a system is first scanned for viruses.

3.10 All MHS IS users are to report suspected virus activity to the local supervisor or IAO. Suspicious activity includes, but is not limited to:

a. Suspected misuse or unauthorized use of government resources.

b. Use of an IS account and password by another party.

c. Illegal copying of software.

d. Abnormal activity on an IS, which may indicate the presence of a computer virus or malicious code.

3.11 Only approved, virus scanned software shall be installed on workstations.

3.12 No software that changes the security posture shall be installed on MHS ISs without approval from the appropriate Designated Approving Authority.

3.13 The IAO shall ensure that backup copies of protected system files, critical data files, and applications (backup copies of applications for archival purposes generally do not represent a copyright violation) are created and stored on electronic storage media in a secure location and are not collocated with the originals. A network/system administrator should have a backup copy of every software program each time it is modified in accordance with established software development procedures and controls. This provides some assurance that a clean backup exists in the event a virus or malicious code is detected. The system administrators should also periodically scan the servers for viruses or malicious code.

3.14 The IAO shall ensure encryption and decryption standards are in compliance with the FIPS Pub 140-2 and DoDI 8500.2. The IAO shall require and ensure encryption policies and procedures are documented.

3.15 Users shall not use electronic storage media from home systems or other external sources that have not been approved and scanned for viruses. Users shall not duplicate copyrighted software or share software with other employees.

3.16 In case of an incident or catastrophic failure, routine data backup and detailed disaster recovery plans shall be available to retrieve exact copies of lost data and ensure data integrity.

3.17 Users shall be trained annually, at the minimum, on appropriate security practices for operating an MHS workstation and IS. Security practices include guarding against, detecting, and reporting malicious software, as well as monitoring and reporting unauthorized logon attempts.

4 REFERENCES

a. CNSSI No. 4009, “National Information Assurance (IA) Glossary,” May 2003

b. CJCSM 6510.01, “Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND),” March 25, 2003

c. DoDI 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997

d. DoDD 5500.7, “Standards of Conduct,” August 30, 1993

e. DoD 5500.7-R, “Joint Ethics Regulation (JER),” August 1993 (Changes 1-4)

f. DoDD 8500.1, “Information Assurance (IA),” October 24, 2002

g. DoDI 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003

h. Federal Information Security Management Act of 2002

i. FIPS Publication 140-2, “Security Requirements for Cryptographic Models,” December 3, 2002

j. NIST SP 500-170, “Management Guide to the Protection of Information Resources,” October 1989

k. NIST SP 800-27, “Engineering Principles for Information Technology Security (A Baseline for Achieving Security),” Revision A, June 2004

l. NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems,” September 2002

m. Public Law 104-191, “Health Insurance Portability and Accountability Act of 1996,” August 21, 1996

n. “DoD Web Site Administration Policies and Procedures,” November 25, 1998, as amended on January 11, 2002

5 ACRONYMS

DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
FIPS	Federal Information Processing Standard
IA	Information Assurance
IAO	Information Assurance Officer
IS	Information System
JMISO	Joint Medical Information Systems Office
MHS	Military Health System
PEO	Program Executive Office
TMA	TRICARE Management Activity
TRO	TRICARE Regional Offices
User ID	User Identification